

PATENT
03000-P0003C TMO/SBS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re The Application Of

Wesley W. Whitmyer, Jr.

Serial No.: 09/706,651

Filed: November 6, 2000

For: On-Site Backup for Internet-Based Data Processing

Examiner: Miranda Le

Group Art Unit: 2177

Confirmation No. 8608

Appeal Brief Under 37 C.F.R. §1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED

MAY 21 2004

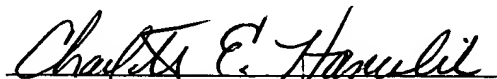
Technology Center 2100

Dear Sir:

Having filed herewith a Notice of Appeal from the final rejection of Claims 1-15, all of the claims currently pending, the final rejection being mailed on April 7, 2004, Appellant submits its Appeal Brief for the above-captioned application pursuant to 37 C.F.R. §1.192 in triplicate as follows:

Certificate of Mailing: I hereby certify that this correspondence is today being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: : Mail Stop Appeal Brief - Patents; Commissioner for Patents; P.O. Box 1450; Alexandria, VA 22313-1450.

May 14, 2004


Charlotte E. Hanulik

Appeal Brief
US Patent Application Serial No. 09/706,651
Filed: November 6, 2000

Real Parties in Interest

The real party in interest is Wesley W. Whitmyer, Jr., 198 Old Kings Highway South, Darien, CT 06820.

Related Appeals and Interferences

There are no related appeals or interferences.

Status Of Claims

Claims 1-15 are currently pending, stand rejected and are the subject of the instant Appeal. A copy of each of these claims is attached hereto as Exhibit A.

Status Of Amendments

Subsequent to the Final Rejection being mailed on April 7, 2004, Appellant has filed no Amendments.

Summary Of Invention

As described in the specification, the claimed invention relates to a system and method for generating and saving a data backup of client data , and more particularly to a data backup system that may be activated by clients for backup of

Appeal Brief
US Patent Application Serial No. 09/706,651
Filed: November 6, 2000

their data contained on a central computer such that a data backup of the client data to be saved is transferred from the central computer to the client computer and is saved thereon. (see e.g., p. 5, lines 4 – 16; p. 6, lines 3 – 10; Figures 1 and 4).

References Cited And Applied

U.S. Patent No. 6,571,280 to Hubacher et al.

U.S. Patent No. 6,574,733 to Langford et al.

Grounds Of Rejection

Claims 1-15 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Hubacher et al. in view of Langford et al.

Issues Presented For Review

(1) Whether a rejection is proper under 35 U.S.C. 103(a) when even if the references are combined and modified as suggested by the Examiner, the resulting combination does even hint at the elements of the claims.

Grouping of Claims

The claims do not stand or fall together. Independent Claims 1, 4, 7 and 10 are directed to the transmission of a data backup to the client computer

aspect of the present invention. While each of Claims 1, 4, 7 and 10 is directed to the same transmission of a data backup to the client computer aspect of the invention, each claims the inventive aspect from a different perspective, and each defines the invention in materially different terms.

Independent Claim 7 is further directed to the data format conversion aspect of the present invention. This claim requires completely different elements as compared to the claims directed only to the transmission of a data backup to the client computer aspect of the invention.

Each of the dependent claims adds specific additional elements to the novel combination of the independent claims. As such, all claims must be considered because it is improper to fail to consider any limitation in the claims. *In re Geerdes*, 491 F.2d 1260, 1262, 180 U.S.P.Q. 789, the 791 (CCPA 1974) (“every limitation in the claim must be given effect rather than considering one in isolation from the others”).

Argument

In an effort to improve customer service, companies are increasingly moving their data processing systems onto the Internet and providing web

interfaces for their customers to see and manipulate their own data. Companies are also outsourcing data processing for their own customers to third parties who, for example, develop and host the companies' web sites.

One difficulty companies face when considering whether to outsource data-processing to third party Internet-based systems is the safeguarding of their and their clients' data. This problem is exacerbated when the company has a duty or professional responsibility to safeguard the data, such as a publicly traded company, law firm or medical practice. Another difficulty companies face in considering to outsource is continuity of service if, for example, the third party were to go out of business.

Many companies who currently perform their own data processing and are sensitized to the need to safeguard their and their customers' data have recently connected their LANs to the Internet, and are beginning to use third-party, Internet-based backup services. This provides a prudent off-site backup but does not offer the benefits of outsourcing the data processing to the Internet. Internet-based application service providers, so-called "ASPs" are also known. User data may be stored on the internet site, however, the data is still entered and manipulated by each user on his LAN/computer and the data manipulation and reporting is handled by each user on his LAN/computer.

Claims 1, 4, 7 and 10 of the present invention are concerned with solving this problem.

More specifically, Claims 1, 4 and 7 each require, among other elements software executing on said central computer for transmitting a data backup to a client computer for onsite backup of internet-based data on the client computer. Claims 1 and 7 further require software executing on the central computer for receiving a data backup request from the client computer, while Claim 4 further requires software executing on the central computer for receiving a reply to the data backup request.

Claim 10 similarly requires, among other elements i) a client data request, sent from the client computer via the Internet to the central computer; and ii) client data corresponding to the client data request, sent from the central computer via the Internet to the client computer and saved on the client computer.

Accordingly, each of the claims are directed to a data backup request sent from the client computer to the central computer and a corresponding data backup sent to and saved on the client computer.

There are a number of ways that the backup request may be sent to the central computer. For instance, the client computer may be set up to pull the

data backup from the central computer by sending a backup request to the central computer each time the client wishes a data backup to be sent to the client computer. Alternatively, the client may access the central computer set up an automated schedule on the central computer to push the information to the client computer based upon the schedule of backup requests the client selects. Still further, the client may manually access the central computer to send a data request for client data to be transferred to the client computer to be saved thereon. In any event, the source of the request for the data backup is the client computer that either sends a request every time a data backup is desired, or initially sends a data backup request that is repeated according to a schedule.

Neither Hubacher et al. nor Langford et al. discloses, teaches or suggests at least the above-highlighted elements. Hubacher et al. is directed to a system for mapping and remapping of drive paths for saved data having redundant file locations. (Hubacher et al., abstract). While Hubacher et al. teaches use of a backup IFS driver for determining the location of backed-up files, it fails to teach “transmitting said data backup to said client computer for onsite backup of internet-based data on said client computer” as required by claims 1, 4 and 7 or client data corresponding to the client data request, sent from the central computer via the Internet to the client computer and saved on the client computer

as required by claim 10. The Examiner has submitted that this limitation is disclosed by Hubacher et al., at for instance Col. 6, lines 12-64 (Official Action 12/19/03) and more specifically at Col. 6, lines 15-30 (Official Action 4/7/04). However, Applicant respectfully submits that this section teaches that “the process starts with the operating system receiving a file request” (col. 6, lines 15-6), the “system then calls the backup IFS driver” (col. 6, lines 19-20), further “the IFS driver reads a file redirection table contained within the backup IFS driver for the requested file” (col. 6, lines 21-2), and then “remaps a destination path in accordance with the destination location for the requested file contained in the file redirection table.” (col. 6, lines 24-6). Nowhere however, does Hubacher et al. teach that the central computer transmits a data backup to the client computer to backup the client data on the client computer. In contrast with the claim language, Hubacher et al. teaches that with “a data backup request, the data is automatically backed up by multiple servers” and is not sent to the client computer and saved thereon as required by all of the claims. (col. 6, lines 27-35 and 56-8; FIGS. 1 and 6) (“In the case of a read request, the backup IFS driver sequentially directs read file requests to a plurality of servers.”)

Hubacher et al. is generally directed toward a searching and updating function for different drive paths on the various system servers where a client data backup is saved. (col. 6, lines 26-40). Nowhere however, does Hubacher et

al. teach that a data backup is sent to the client computer for onsite backup on the client computer or that client data corresponding to the client data request, is sent from the central computer via the Internet to said client computer and saved on said client computer.

The examiner has submitted that Hubacher et al. teaches these limitations. Applicant respectfully disagrees. In an Official Action dated 4/7/04 at pages 9 and 10 the Examiner stated “that Hubacher discloses these servers provide data (i.e. data backup), such as boot files, operating system, images, and applications to clients 108, 110, 112 (col. 3, lines 21-24)” and that “[i]t should be understood that “read request” corresponds to a data backup request from a client computer.” The Examiner then stated that a “read request” or a request to access data on the central computer is the same as a data backup sent from the central computer to the client computer and saved thereon. In that same Official Action on page 11 however, the Examiner later waffled on this point stating that “[i]t should be noted that since servers 104, 114, 116, 118 provide data (i.e. data backup) ... these files should be saved on the client computer.” (emphasis added). Hubacher et al. however does not teach these limitations.

Applicant disagrees with the Examiner’s position that allowing a client to simply read data stored on a system server equates to transmitting a data backup to a client computer for onsite backup of internet-based data on the client

computer. Merely allowing access to read information is not that same as transmitting a data backup to a client computer and storing the data backup on the client computer. Even the Examiner's comments that "these files should be saved on the client computer" shows that the Examiner even now has not been able to locate this limitation in Hubacher et al. (emphasis added).

The Examiner has also submitted in an Official Action dated 4/7/04 at page 10 that once the path is determined by the system the "backup IFS then remaps a destination path in accordance with the destination location (i.e. client computer) for the requested file (col. 6, lines 21-26)." This misstates the teaches of Hubacher et al. which never teaches or discloses that the backup IFS remaps a destination path to a client computer, rather all of the data backups are stored exclusively on the various system servers, never on a client computer as suggested by the Examiner. (col. 6, lines 20-22, 27-40). While the Examiner has submitted that Hubacher et al. "is directed to a method and apparatus for client sided backup" (emphasis in original), the Examiner has failed to show where in Hubacher et al. the limitations of transmitting said data backup to said client computer for onsite backup of internet-based data on said client computer, or client data corresponding to said client data request, sent from said central computer via the Internet to said client computer and saved on said client computer is taught as required by all of the claims of the present application.

Applicant respectfully submits that the Examiner has not cited Langford et al. as teaching these claim elements and Applicant submits that Langford et al. does not teach these limitations.

Storing the data backup on the client computer and not solely on the network of servers allows the present invention to solve a problem that neither Hubacher et al. nor Langford et al. can solve. For instance, Hubacher et al. teaches saving the data on multiple servers that are searchable with a backup IFS driver. While this may protect the data if something adverse happens to one of the servers, this will not protect the data if the company providing the server storage, for instance, goes out of business. Another advantage of having a local copy of the data stored on the client computer is if the client's Internet connection is interrupted, the client is still able to operate as he has a local copy of his data. Still further, some professionals have a professional responsibility to ensure that their data is safe and accessible whenever needed and may not be comfortable relying on their Internet connection to fulfill this responsibility. Having the ability to redundantly save a data backup on the client computer will provide the client with greater peace of mind knowing that critical data is protected by more than one company's system. This benefit however, cannot be realized by Hubacher et al. or by Langford et al. because there is no transmission of a data backup to

Appeal Brief
US Patent Application Serial No. 09/706,651
Filed: November 6, 2000

the client computer for onsite backup of internet-based data on the client computer.

Claims 1 and 7 further require among other elements “software executing on said central computer for receiving a data backup request from said client computer” while claim 10 requires among other elements “a data backup request, sent from said client computer via the Internet to said central computer.” The Examiner has submitted that this element is disclosed by Hubacher et al. at col. 6, lines 15-30 and col. 7, lines 12-22. Applicant respectfully disagrees.

Hubacher et al. teaches a “local request” which may comprise a “read request to \\Server1\alias\config.sys” and that if “Server1 fails to respond, the backup IFS driver directs the request to \\Server2\alias\config.sys. If that server fails to respond, the backup IFS driver directs the read request to x:\config.sys.” (col. 7, lines 15-9). These sections cited by the Examiner however are examples of read requests sent by the client, not data backup requests. Again, Hubacher et al. is concerned with the mapping and remapping of saved data on various system servers and retrieving that information for the client during a “read request.” While Hubacher et al. may teach a “local request” or a “read request”, it does not teach a data backup request sent from the client computer to the central computer.

The system taught and claimed in the present application is directed toward a backup system that may be activated by clients for backup of their data contained on a central computer, such that a data backup is transferred from the central computer to their computer or network. As previously mentioned, there are a number of ways that the backup request may be sent to the central computer including automatically or manually pulling the data from the central computer or pushing the data to the client computer. In any event, the source of the request for the data backup is the client computer that either sends a request every time a data backup is desired, or initially sends a data backup request that is repeated according to a schedule. Neither of these methods are taught by Hubacher et al. or Langford et al., both of which fail to teach transferring any type of data backup from a central computer to a client computer.

Claim 7 still further requires among other elements "software executing on said central computer for receiving a data backup request and for receiving a data format conversion request" and "software executing on said central computer for retrieving said data from said database and for converting said data to a format corresponding to said data format conversion request." The Examiner has submitted that these limitations are taught by Langford et al. at col. 3, lines 9-27. Applicant respectfully disagrees. While Langford et al. discusses a

Appeal Brief
US Patent Application Serial No. 09/706,651
Filed: November 6, 2000

“backup data encryptor” and that the “centralized secure data backup processor 12 centrally initiates extraction of data from the data sources 20a-20n for data that is to be backed-up based on for example, centralized backup policy data”, nowhere is “a data format conversion request” identified. In addition, nowhere does Langford et al. teach converting the data to a format corresponding to the data format conversion request as required by claim 7. Rather, the present invention solves a problem that Langford et al. cannot solve, namely the “additional feature allows a client to back-up data on-site that is securely stored in a plurality of formats the client may require.” (p. 6, lines 4-6).

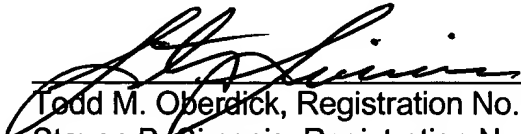
Appeal Brief
US Patent Application Serial No. 09/706,651
Filed: November 6, 2000

Conclusion

Appellant has made a significant advance over the prior art by providing an improved system and method for providing data backups of sensitive client data, and more particularly to a system and method which provides onsite security of critical data saved on the client computer, which allows for instance, a company with a professional responsibility to effectively safeguard the data. Accordingly, reconsideration and allowance of all pending claims is believed in order, and such action is earnestly solicited.

Respectfully submitted,

May 13, 2004



Todd M. Oberdick, Registration No. 44,268
Steven B. Simonis, Registration No. 54,449
ST. ONGE STEWARD JOHNSTON & REENS
986 Bedford Street
Stamford, Connecticut 06905
(203) 324-6155

Attorneys for Appellant

Copy of the Claims

1. (previously amended) A system for onsite backup of internet-based data comprising:
 - a central computer;
 - a client computer;
 - a communications link between said central computer and the Internet;
 - a communications link between said client computer and the Internet;
 - at least one database containing a plurality of data records accessible by said central computer, each data record containing a client identification number;
 - software executing on said central computer for receiving a data backup request from said client computer;
 - software executing on said central computer for transmitting said data backup to said client computer for onsite backup of internet-based data on said client computer.
2. (previously amended) The system of claim 1 further comprising of software executing on said client computer for storing said data backup in a location accessible to said client computer.
3. (original) The system of claim 2 further comprising of software executing on said central computer for retrieving said data backup.
4. (previously amended) A system for onsite backup of internet-based data comprising:
 - a central computer;
 - a client computer;

a communications link between said central computer and the Internet;
a communications link between said client computer and the Internet;
at least one database containing a plurality of data records accessible by said central computer, each data record containing a client identification number;
software executing on said central computer for receiving commands from said client computer;
software executing on said central computer for receiving data from said client computer;
software executing on said central computer for storing said received data in said database;
software executing on said central computer for generating a data backup request;
software executing on said central computer for transmitting said data backup request through the internet;
software executing on said central computer for receiving a reply to said data backup request;
software executing on said central computer for transmitting said data backup to said client computer for onsite backup of internet-based data on said client computer.

5. (original) The system of claim 4 further comprising of software executing on said client computer for storing said data backup in a location accessible to said client computer.

6. (original) The system of claim 4 further comprising of software executing on said central computer for retrieving said data backup.

7. (previously amended) A system for onsite backup of internet-based data comprising:

- a central computer;
- a client computer;
- a communications link between said central computer and the Internet;
- a communications link between said client computer and the Internet;
- at least one database containing a plurality of data records accessible by said central computer, each data record containing a client identification number;
- software executing on said central computer for receiving commands from said client computer, for receiving data from said client computer, and for storing said data in said database;
- software executing on said central computer for receiving a data backup request and for receiving a data format conversion request;
- software executing on said central computer for retrieving said data from said database and for converting said data to a format corresponding to said data format conversion request;
- software executing on said central computer for encrypting said data backup;
- software executing on said central computer for transmitting said data backup to said client computer for onsite backup of internet-based data on said client computer; and
- software executing on said client computer for decrypting said data backup.

8. (original) The system of claim 7 further comprising of software executing on said client computer for storing said data backup in a location accessible to said client computer.

9. (original) The system of claim 7 further comprising of software executing on said central computer for retrieving said data backup.

10. (previously added) A system for local storage of data through the Internet comprising:

- a central computer connected to the Internet;

- a client computer connected to the Internet;

- at least one storage having a plurality of client data records, said at least one storage accessible by said central computer, each client data record having an identifier that relates the client data record to a client;

- a client data request, sent from said client computer via the Internet to said central computer; and

- client data corresponding to said client data request, sent from said central computer via the Internet to said client computer and saved on said client computer.

11. (previously added) The system according to claim 10 wherein said client data is encrypted prior to being sent to said client computer to be saved thereon.

12. (previously added) The system according to claim 10 further comprising a data format conversion request, sent from the client computer to said central computer.

13. (previously added) The system according to claim 12 wherein said central computer converts said client data to a format corresponding to said data format conversion request.

Appeal Brief
US Patent Application Serial No. 09/706,651
Filed: November 6, 2000

14. (previously added) The system according to claim 13 wherein the conversion of said client data to a format corresponding to said data format conversion request occurs prior to said client data being sent from the client computer to said central computer.

15. (previously added) The system according to claim 12 wherein said client data is encrypted prior to being sent to said client computer to be saved thereon.